Department of Defense

DIRECTIVE

NUMBER 8581.1E
June 21, 2005

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA) Policy for Space Systems Used by the Department of Defense

References: (a) National Security Directive 42[1], "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
(b) National Security Telecommunications and Information System Security Policy No. 12[2], "National Information Assurance (IA) Policy for U.S. Space Systems," January 2001
(c) DoD Directive C-3100.9, "Space Systems Policy (U)," March 28, 1977 (hereby canceled)
(d) DoD Directive 8500.1, "Information Assurance," October 24, 2002
(e) through (x), see enclosure 1

1. PURPOSE

This Directive:

1.1. Implements the requirements of reference (a) by establishing Information Assurance (IA) policy and assigning IA responsibilities for all DoD space systems in accordance with reference (b).

1.2. Supersedes and cancels reference (c).

1.3. Supplements IA policy and requirements contained in reference (d) and DoD Instruction 8500.2 (reference (e)).

[1] Available at http://www.iad.nsa.smil/library
[2] Available at http://www.nstissc.gov/html/library.html

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.1.2. All types of DoD-owned or controlled space systems, and the components thereof, that collect, generate, process, store, display, transmit, or receive national security or DoD sensitive information (e.g., launch vehicles, satellites, payloads, launch and test ranges, satellite and network operation centers, and user equipment).

2.1.3. Commercial (domestic and foreign), U.S. civil, or foreign government-owned (i.e., those not owned or controlled by the Department of Defense) space systems, components, or services used by the Department of Defense to collect, generate, process, store, display, transmit, or receive national security or DoD sensitive information.

2.1.4. Interfaces between space systems covered by this Directive and external systems when it is determined that the architecture of the space system does not provide for adequate protection against potential threats from interconnected, external systems.

2.2. This Directive does not apply to the following:

2.2.1. Aircraft, operational ballistic missile weapons systems, anti-ballistic missile systems, munitions, and suborbital test vehicles that do not have subsystems that are part of a space system. When subsystems exist that are part of a space system, this Directive shall specifically apply to those subsystems.

2.2.2. DoD-owned or controlled space systems or segments thereof that were past the point of program initiation when this Directive became effective with the following exceptions, or as noted in section 4.

2.2.2.1. This exemption does not automatically apply to any subsequent major redesigns of these systems or segments. Program Managers shall request that the DoD Executive Agent for Space review proposed major redesigns of legacy systems and decide if this Directive should apply. The DoD Executive Agent for Space (DoD Directive 5101.2 (reference (f)) shall consult with the Commander, U.S. Strategic Command, and the Director, National Security Agency (DIRNSA), prior to making a decision.

2.2.2.2. The DoD Executive Agent for Space, in consultation with the Commander, U.S. Strategic Command, and the DIRNSA, may revoke this exemption on a case-by-case basis for programs past the point of program initiation, but still in development, if the potential IA-related risks to the space system clearly outweigh the cost and schedule impact of fully complying with this Directive.

2.2.3. Commercial, U.S. civil, or foreign-owned space systems providing services to the Department of Defense that were already under lease or other use agreement when this Directive became effective for the life of the current lease or use agreement.

2.3. The scope of this Directive includes the policy, planning, budgeting, requirements generation, research, development, testing, evaluation, production, acquisition, deployment, maintenance, life cycle support, education, training, exercises, operations, employment, and oversight of IA activities that are integral to the space systems used by the Department of Defense. DoD information and data that transit space systems shall be protected (e.g., encryption for confidentiality) in accordance with references (d) and (e).

2.4. Nothing in this policy shall alter or supersede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference (g)) and other laws and regulations.

3. DEFINITIONS

Terms used in this Directive are defined in Committee on National Security Systems Instruction No. 4009 (reference (h)) or in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. All DoD-owned or controlled space systems shall meet the following system specific IA requirements regardless of mission assurance category (MAC) or classification:

4.1.1. IA requirements for all DoD-owned or controlled space systems shall be defined and updated throughout the system life cycle consistent with the IA Component of the Global Information Grid (GIG) architecture and in coordination with the DIRNSA, space system program offices, the system Designated Approving Authority (DAA), and sustainment organizations after considering the current and projected full-range of threats to space systems based on threat information provided by the Director of the Defense Intelligence Agency. IA requirements for systems supporting Joint and Combined operations shall be validated through the Joint Requirements Oversight Council. IA requirements for all other systems shall be validated through the appropriate Service Requirements Oversight Council. Both the selecting

and implementing of cryptography used to meet IA requirements shall be approved by the DIRNSA.

4.1.2. IA shall be applied in a balanced manner by performing Information System Security Engineering (ISSE) as an integral part of the space system architecture and system engineering process to address all IA requirements in the intended operational environment. Defense-in-depth measures shall be designed into space systems and include deterrence, detection, recovery, and reporting capabilities to: counter attacks or security lapses; detect, characterize, and locate the source of an attack; recover from any damage sustained; and quickly alert command authorities via secure communications of any security lapses or attacks. These IA measures help ensure mission success and contribute to satisfying the GIG policy requirements in DoD Directive 8100.1 (reference (i)).

4.1.3. The command links to DoD-owned or controlled space platforms shall be encrypted and authenticated on an end-to-end basis using National Security Agency (NSA)-approved cryptography.

4.1.4. Data generated onboard space platforms (e.g., telemetry and mission data) shall be end-to-end encrypted using NSA-approved cryptography.

4.1.5. All links (e.g., command uplinks, downlinks, and crosslinks) on DoD-owned or controlled space systems, regardless of transmission media (radio frequency, optical, etc.), shall have transmission security (TRANSEC) protection (e.g., anti-jam and traffic flow security) appropriate for the mission and the projected threat environment over the life of the system. The TRANSEC protection measures used shall be reviewed and approved by the DIRNSA for the intended application.

4.1.6. Booster telemetry links shall not be encrypted. Emergency, backup links that are automatically invoked to rectify lost communications with malfunctioning satellites need not be encrypted.

4.1.7. A Flight Termination System that uses a Secure Command Destruct System employing NSA-approved cryptography shall be required for all launch vehicles used to deploy DoD-owned or controlled space platforms.

4.1.8. Any capability designed into DoD-owned or controlled space systems to bypass, for any reason, link protection measures required by this policy during system operation shall minimize the probability of bypass activation due to either malicious acts or random failures. The bypass design shall be submitted to the DIRNSA for review and comments early in the preliminary design phase. The bypass design shall be submitted to the DIRNSA for final approval well in advance of the system critical design review to allow the DIRNSA to respond with comments or approval prior to the system critical design review date. Provisions shall also be made for the DIRNSA to review how the bypass was actually implemented in the operational system to ensure that no inadvertent flaws were introduced.

4.1.9. Commercial-off-the-shelf (COTS) IA or IA-enabled information technology (IT) products (i.e., hardware, software, and firmware) being considered for use on DoD-owned or controlled space systems shall be limited to products that have been evaluated and validated in accordance with the requirements of National Security Telecommunications and Information System Security Policy No.11 (reference (j)) or for which waivers have been obtained.

4.1.10. DoD-owned or controlled space systems shall undergo IA certification and accreditation (C&A) in accordance with DoD Instruction 5200.40 (reference (k)).

4.1.11. Interconnections of Intelligence Community (IC) systems with DoD space systems shall be certified and accredited in accordance with a process jointly developed by the DoD Chief Information Officer (CIO) and the IC CIO. For those space systems that transmit, store, or process SCI or other intelligence information under the purview of the DCI, the C&A requirements of DCI Directive 6/3 (reference (l)) shall apply.

4.1.12. The interconnection of DoD space systems with systems of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and, whenever possible, DoD IA policies. Variations shall be approved by the responsible Combatant Commander and the DAAs, and incorporated in the IA C&A package. Prior to agreeing to such interconnections, the DIRNSA shall be contacted regarding the releasability of any cryptographic equipment, key, or technology that may be involved.

4.1.13. Each DoD-owned or controlled space system covered by this policy shall have a DAA, Certification Authority (CA), and User Representative formally assigned. Additionally, legacy space systems shall have a DAA assigned to adjudicate any significant IA issues that may arise.

4.1.14. The status of the IA C&A package and IA-related deliverables shall be a required review item for all major acquisition milestone reviews beginning with the key decision point associated with approval to enter into risk reduction and design development activities.

4.1.15. IA shall be a visible element of all space system investment portfolios. Data shall be collected to support reporting and IA management activities across the investment life cycle.

4.1.16. Every DoD-owned or controlled space system shall have a continuity of operations plan and procedures that account for the availability of backup capabilities to support DoD space system operations.

4.2. All commercial, U.S. civil, or foreign government-owned space systems (i.e., those not owned or controlled by the Department of Defense) used by the Department of Defense to collect, generate, process, store, display, transmit, or receive national security or DoD sensitive information shall meet the following IA requirements:

4.2.1. U.S. commercial and civil land remote sensing satellites, as well as communications, weather, and navigation space systems leased or used by the Department of

Defense for national security purposes shall employ NSA-approved cryptography to encrypt and authenticate commands to the space system if supporting MAC I or II systems. While NSA-approved cryptography is preferred for MAC III systems, cryptography generally commensurate with commercial best practices is acceptable for encrypting and authenticating commands to MAC III space systems.

4.2.2. Data and Imagery Protection:

4.2.2.1. The DoD Components shall acquire commercial remote sensing data, imagery, products, or services that use commercial remote sensing systems with IA equipment, policies, and procedures that are commensurate with the confidentiality level (i.e., classified, sensitive, or public) of the data, imagery, products, or services to be obtained. This shall include protecting both upper-tier data and imagery, and also exclusive U.S. Government (USG) use and access data and imagery.

4.2.2.2. DoD organizations that contemplate developing a remote sensing system jointly with a commercial remote sensing operator shall consult with the DIRNSA for guidance on those IA protection measures that would be appropriate given the sensitivity of the data, imagery, products, or services to be provided by the new system.

4.2.3. Foreign government-owned systems do not require the use of on-board DIRNSA-approved cryptography for the Department of Defense to use them.

4.2.4. The Department of Defense shall give preference to leasing or acquiring data, imagery, products, or services from those commercial, U.S. civil, or foreign government-owned space systems that incorporate additional IA measures beyond the minimum specified in this Directive which substantially improve system availability and the protection of national security or DoD sensitive information.

4.2.5. Any capability designed into commercial, U.S. civil, or foreign government-owned space systems providing services to the Department of Defense that allows the bypass of any DIRNSA-approved cryptography shall minimize the probability of bypass activation due to malicious or unintentional acts or random failures. The satellite system owner or operator shall submit the bypass design and implementation details to the DIRNSA for review and comments early in the preliminary design phase. The bypass design shall be submitted to the DIRNSA for final approval in advance of the system critical design review to allow the DIRNSA to respond with comments or approval prior to the system critical design review date. Once approved by the DIRNSA, the record of this approval shall be made available to the responsible DAA in support of the DAA's risk management decision regarding whether to lease or negotiate use of a commercial, U.S. civil, or foreign government-owned space system to support national security or sensitive missions. Evaluation and approval of encryption bypasses not specifically under the control of the satellite owner and operator (e.g., teleports and communications earth stations not operated by the satellite operator) shall be performed separately from this evaluation.

4.3. A Cryptographic Security Plan shall be required in accordance with reference (b) for all space systems covered by this Directive if they have NSA-approved cryptography.

4.4. Waivers to specific policy requirements of this Directive may be granted by the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) on a case-by-case basis. Waiver requests on national policy requirements shall be handled by the ASD(NII) in accordance with reference (b).

4.4.1. Requests shall be sent through the organization's chain of command and the appropriate DAAs. Each shall indicate their approval or disapproval of the request. If all approve, the request shall be forwarded to the DIRNSA; otherwise, it shall be returned to the originator with an explanation for the disapproval. (See enclosure 3).

4.4.2. The DIRNSA shall request and review any pertinent information from DoD and IC organizations in developing and providing a recommendation on a waiver request to the ASD(NII)/DoD CIO, as appropriate. The ASD(NII)/DoD CIO may adjudicate waivers when operational needs dictate expeditious handling to support planned or on-going operations. However, the adjudication must be done in consultation with the DIRNSA; the Commander, U.S. Strategic Command; and the DoD Executive Agent for Space. Consultation with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) is also required when the USD(AT&L) is the Milestone Decision Authority (MDA) or when the MDA reports to the USD(AT&L).

4.4.2.1. Each organization receiving a waiver request shall provide their operational and technical assessments along with recommendations to the DIRNSA for consolidation and review.

4.4.2.2. Each organization shall evaluate requested waivers to this Directive to determine how the waivers, if granted, will result in avoiding unacceptable or adverse impacts on mission, operational plans, and orders; cost or schedule impacts that are determined to be excessive relative to the protection afforded; or any inappropriate or unnecessary protection requirements.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall:

5.1.1. Monitor all IA activities related to space systems used by the Department of Defense.

5.1.2. Perform, as needed, an independent evaluation of IA program performance and resource availability to ensure the implementation of the overall space IA program related to the Department of Defense's use of space systems. This shall be accomplished through examination

of the adequacy of the NSA's and the DoD Components' IA budgets to ensure the life cycle protection of space systems used by the Department of Defense.

5.1.3. Adjudicate requested waivers to the DoD-unique policy requirements of this Directive.

5.1.4. Oversee the assignment of User Representatives, MAC levels, and confidentiality levels to space systems covered by this policy.

5.1.5. Direct the Director, Defense Information Systems Agency (DISA) to:

5.1.5.1. Ensure that solicitations, contracts, or formal agreements under DISA's purview to acquire satellite communications services from commercial, U.S. civil, or foreign government-owned space systems contain specific IA-related language and requirements to comply with this Directive.

5.1.5.2. Coordinate with the DIRNSA to obtain guidance, advice, and current information to assist with developing appropriate IA-related language for such solicitations, contracts, or formal agreements.

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics, when serving as the MDA of space systems or systems that interact with space systems, shall:

5.2.1. Monitor and provide oversight, including IA. This shall include independent evaluations of program performance and resource requirements.

5.2.2. Coordinate IA-related activities with the ASD(NII)/DoD CIO.

5.3. The Under Secretary of Defense for Intelligence shall:

5.3.1. Ensure that the Director, National Security Agency, reporting to the ASD(NII) for IA matters, shall:

5.3.1.1. Keep the ASD(NII)/DoD CIO and the DoD Executive Agent for Space apprised of all IA initiatives and activities impacting DoD Space Programs.

5.3.1.2. Plan, budget for, and perform IA-related research and technology development needed to protect future space systems likely to be developed and/or used by the Department of Defense and coordinate those activities with the Director, Defense Research and Engineering.

5.3.1.3. Oversee the planning, development, and production of space-specific cryptography for which the DIRNSA has certification responsibility.

5.3.1.4. Develop and produce cryptographic components for space when requested and funded per agreement between the DIRNSA and the Heads of the DoD Components.

5.3.1.5. Review and approve, as appropriate, the DoD Component proposals to initiate and manage the development of cryptographic products for space systems. Provide oversight and technical guidance to approved cryptographic development efforts leading up to the DIRNSA's evaluation and certification.

5.3.1.6. Provide guidance to the ASD(NII)/DoD CIO and the DoD Components on the acquisition, integration, and life cycle support of IA products, services, measures, and techniques into space systems used by the Department of Defense.

5.3.1.7. Provide ISSE support and guidelines to DoD space system programs beginning with concept and technology development, and continuing throughout their life cycle to assist and help guide DoD space program efforts.

5.3.1.8. Review, approve, and provide guidance on, or perform the evaluation and certification of all cryptographies or other means that are intended to provide equivalent or greater levels of protection to satisfy the IA requirements associated with this policy.

5.3.1.9. Evaluate and certify the implementation, integration, and/or embedment of cryptography into DoD-owned or controlled space systems. Provide data on this cryptography-related evaluation and certification to the system CA to support certifying the overall security of the space system.

5.3.1.10. Perform end-to-end, system security evaluations on space systems used by the Department of Defense when requested by the ASD(NII)/DoD CIO, the DoD Executive Agent for Space, the USD(AT&L), or the Commander, U.S. Strategic Command, to assist in identifying IA-related vulnerabilities, assurances, threats, and risks.

5.3.1.11. Provide IA advice and assistance to DoD space-related acquisition and operational components planning to contract for the design, development, manufacture, acquisition, lease, launch, or operation of any space system to be used by the Department of Defense.

5.3.1.12. Provide guidance on the use of COTS IA or IA-enabled IT products (i.e., hardware, software, and firmware) being considered for application in space systems to be used by the Department of Defense.

5.3.1.13. Review and process requests for waivers to this Directive, including justification and explanatory details, and provide appropriate recommendations to the ASD(NII)/DoD CIO for consideration.

5.3.1.14. Review and provide comments and recommendations to the DoD Executive Agent for Space, as requested, regarding extending the applicability of this Directive to systems past the point of program initiation or to legacy systems that are undergoing major redesign.

5.3.1.15. Ensure the full inclusion of space systems IA architectures within the IA component of the overall GIG architecture.

5.3.1.16. Maintain reports and other pertinent information provided by commercial, U.S. civil, and foreign government-owned space system owners or service providers describing the IA measures taken to protect their systems.

5.3.2. Direct the Director, Defense Intelligence Agency to prepare and update the current and projected full-range of threats, to include information operations threats, to space systems and provide a report annually on January 31st to the ASD(NII)/DoD CIO; the Commander, of the U.S. Strategic Command; the DoD Executive Agent for Space; the USD(AT&L); and the DIRNSA.

5.3.3. Direct the Director, National Geospatial-Intelligence Agency (NGA) to:

5.3.3.1. Ensure solicitations, contracts, or formal agreements under the NGA Director's purview to acquire remote sensing services from commercial, U.S. civil, or foreign government-owned space systems contain specific IA-related language and requirements to comply with this Directive. The NGA Director shall coordinate with the DIRNSA to get guidance, advice, and current information to assist with developing appropriate IA-related language for such solicitations, contracts, or formal agreements.

5.3.3.2. Ensure commercial remote sensing system IA equipment, policies, and procedures are commensurate with the confidentiality level of the data, imagery, products, or services acquired.

5.4. The DoD Executive Agent for Space shall:

5.4.1. Decide on a discretionary basis, in consultation with the Commander, U.S. Strategic Command, and after coordinating with the Chairman of the Joint Chiefs of Staff, the Heads of DoD Components that have an operational interest, and the system DAA, whether a space system past the point of program initiation, but still in development, or a legacy system undergoing major redesign, shall be subject to the full provisions of this Directive. This decision shall be based primarily on whether the potential IA-related risks of non-compliance outweigh the cost and schedule impact of complying with this Directive.

5.4.2. Provide oversight of all IA activities related to space systems used by the Department of Defense.

5.5. The Heads of the DoD Components shall:

5.5.1. Ensure compliance with the IA requirements of this policy for developing, acquiring, deploying, leasing, operating, and maintaining all space systems that are used by the Department of Defense to collect, generate, process, store, display, transmit, or receive national security and DoD sensitive information, or that perform national security functions throughout their life cycle.

5.5.2. Incorporate IA products, services, measures, and techniques throughout the life cycle of all information systems (ISs) and networks that are integral to or essential for the operation of space systems used by the Department of Defense.

5.5.3. Assign DAAs for all DoD Component-owned or -controlled space systems, including those that are at or beyond the point of program initiation.

5.5.4. Appoint a User Representative for each space system for which they have an operational interest.

5.5.5. Assign MACs and confidentiality levels to space system components under their purview.

5.5.6. Plan, program, budget for, implement, and manage programs for the development, production, acquisition, integration, maintenance, disposal, and/or life cycle support of IA products or operational measures into space systems used by the Department of Defense for which they are responsible.

5.5.7. Ensure, through contractual or formal agreements, that the requirements of this policy are applied to all Government contracts and commercial, U.S. civil, or foreign government entities involved in the deployment, operation, or maintenance of national security space systems used by the Department of Defense. Solicitations, contracts, or formal agreements shall include specific requirements for IA products, reviews, evaluations, services, measures, or techniques, as required by this Directive and mission requirements. Coordinate with the NSA to get guidance, advice, and current information to assist with developing appropriate IA-related language for such solicitations, contracts, or formal agreements.

5.5.8. Ensure COTS IA or IA-enabled IT products being considered for use on DoD-owned or controlled space systems for ensuring total system integrity are limited to products evaluated and approved by the DIRNSA according to the DIRNSA processes or evaluated and validated according to the requirements of reference (i).

5.5.9. Ensure continuity of operations planning and procedures account for the availability of backup capabilities to support DoD space system operations, in the event affected systems are unable to be restored along timelines needed to reconstitute and assure mission support.

5.5.10. Ensure Program Managers for space systems under their purview include performing ISSE and C&A in their program plans, budgets, and contracts, as appropriate.

5.5.11. Coordinate on waiver requests related to this Directive.

5.5.12. Ensure the validation of IA requirements through Service Requirement Oversight Councils as appropriate for space systems that do not support Joint and Combined Operations.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on IA for space systems.

5.6.2. Ensure, in coordination with the ASD(NII)/DoD CIO, the validation of IA requirements for space systems supporting Joint and Combined operations through the Joint Requirements Oversight Council.

5.6.3. Develop, coordinate, and promulgate IA policies, doctrine, and procedures for Joint and Combined space operations.

5.7. The Commander of the U.S. Strategic Command, through the Chairman of the Joint Chiefs of Staff, shall:

5.7.1. In coordination with the system DAA(s), the NSA, and other organizations as appropriate, determine the levels of IA necessary to protect the operations and assets of national security space systems used by the Department of Defense; and periodically test and exercise IA-related procedures, processes, products, services, measures, and techniques.

5.7.2. Advocate and provide recommendations to the Chairman of the Joint Chiefs of Staff on joint computer network defense operations, policy guidance, and capability requirements for space systems.

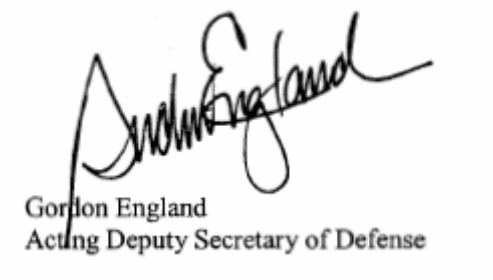
5.7.3. Ensure space systems are included within the IS incident reporting program as a component of DoD-wide incident reporting.

5.7.4. Develop defensive actions necessary to deter or defeat unauthorized activity (e.g., computer network attack and computer network exploitation against DoD-owned or controlled space systems and minimize damage from such activities).

5.7.5. Assign DAAs for all DoD-owned or controlled space systems that support more than one DoD Component, including those that are at or beyond the point of program initiation. This shall be done in coordination with the Chairman of the Joint Chiefs of Staff, the system's MDA, and the Heads of the DoD Components that have an operational interest.

6. EFFECTIVE DATE

This Directive is effective immediately.



Enclosures – 3

E1. References, continued
E2. Definitions
E3. Waiver Request Format

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(f) DoD Directive 5101.2, "DoD Executive Agent for Space," June 3, 2003
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(h) Committee on National Security Systems Instruction No. 4009[3], "National Information Systems Security Glossary," May 2003
(i) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(j) National Security Telecommunications and Information System Security Policy No. 11[4], "National Policy for the Acquisition of Evaluated IA and IA-Enabled COTS Products," January 2000
(k) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997
(l) Director of Central Intelligence Directive 6/3[5], "Protecting Sensitive Compartmented Information Within Information Systems," June 5, 1999
(m) DoD Directive S-3600.1, "Information Operations," December 9, 1996
(n) Chapter 82 of title 5, United States Code, "Land Remote Sensing Policy Act of 1992"
(o) Executive Order 12958, "Classified National Security Information," April 17, 1995
(p) National Security Space Acquisition Policy 03-01, October 6, 2003
(q) Section 552a of title 5, United States Code, "The Privacy Act of 1974"
(r) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998
(s) Section 552 of title 5, United States Code, "Freedom of Information Act"
(t) Section 1514 of title 22, United States Code, "The Arms Export Control Act"
(u) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(v) DoD 5200.1-R, "Information Security Program," January 17, 1997
(w) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UNCI)," November 15, 1991
(x) DoD Directive 3100.10, "DoD Space Policy," July 9, 1999

[3] Available at http://www.nstissc.gov/html/library.html
[4] Available at http://www.nstissc.gov/html/library.html
[5] Available at http://www.cms.cia.sgov.gov

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Accreditation. Formal declaration by a DAA that an IS is approved to operate in a particular security mode at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards (reference (h)).

E2.1.2. Assurance. Measure of the confidence that the security features and architecture of an IS accurately mediate and enforce the security policy (reference (h)).

E2.1.3. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (h)).

E2.1.4. Availability. Timely, reliable access to data and information services for authorized users (reference (h)).

E2.1.5. Certification. Comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meets a set of specified security requirements (reference (h)).

E2.1.6. Certification and Accreditation (C&A) Package. The portfolio of IA documents that are maintained and updated throughout the life cycle of a system starting with program inception to: document IA requirements and guide all IA C&A activities; document decisions and agreements between the DAA, the CA, the User Representative, and the system Program Manager concerning both system developmental and operational IA-related requirements, responsibilities, policies, doctrine, assurances, and solutions; document C&A plans, responsibilities, resources, level-of-effort, test results and recommendations; document system security trades, C&A tailoring, and risk management decisions affecting the IA posture of the system; and document System Security Plans or System Security Authorization Agreements.

E2.1.7. Certification Authority (CA). The official responsible for managing the comprehensive evaluation of the technical and non-technical security features of an IT system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements.

E2.1.8. Command Uplink. Data transmission path established for purposes of positioning or relocating space platforms (i.e., orbital insertions or adjustments), or for effecting tasking changes to the satellite, its subsystems, or mission payload(s).

E2.1.9. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes (reference (h)).

E2.1.10. Crosslink. A data link between space platforms.

E2.1.11. Defense-in-Depth[6]. The DoD approach for establishing an adequate IA posture in a shared risk environment that allows for shared mitigation through the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and the selection of IA solutions based on their relative level of robustness (reference (d)).

E2.1.12. Designated Approving Authority (DAA)[7]. Official with the authority to formally assume the responsibility for operating a system or network at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority (reference (h)).

E2.1.13. DoD-Owned or Controlled Space System. Any space system where development or operation is funded or controlled (e.g., via outsourcing contract) primarily by the Department of Defense to support the DoD mission.

E2.1.14. Downlink. Data link from a space platform to a ground or airborne platform.

E2.1.15. End-to-End IA System Security Evaluation. A comprehensive system analysis via system design and process reviews along with system and component level testing to uncover, identify, and document all IA- related vulnerabilities, weaknesses, and assurances.

E2.1.16. External System. A system that is outside the intrinsic and commonly recognized boundaries of the system of interest (e.g., DoD space system). An example of an external system is a widely shared, communications backbone or data network that a space system might interface with for communications or data services.

E2.1.17. Flight Termination System. A capability designed and incorporated into launch vehicles (and unmanned airborne vehicles) which, in the event of anomalies that might pose a threat to lives, property or the compromise of national security-related technology provides for the termination of the launch process or flights.

E2.1.18. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.

E2.1.19. Information Assurance (IA). Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

---

[6] See the Information Assurance Technical Framework available at http://www.iatf.net for technical guidance with respect to defining defense-in-depth requirements and to identify potential approaches to meet those requirements

[7] Depending on the type of space system, one or more DAAs may be assigned. For example, on a space platform with multiple payloads serving different missions, a different DAA may be appropriate for each payload to reflect its primary owner or operator, in addition to the DAA assigned to the platform itself. For a communications satellite/payload serving many users, a DAA is assigned for the satellite and payload, but individual communication paths through the satellite may be associated with missions that have their own DAA assigned.

This includes providing for restoration of ISs by incorporating protection, detection, and reaction capabilities (reference (d)).

E2.1.20. IA Certification and Accreditation (IA C&A). The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD ISs (reference (f)).

E2.1.21. Information Operations. Actions taken to affect adversary information and ISs while defending one's own information and ISs in accordance with DoD Directive S-3600.1 (reference (m)).

E2.1.22. Information System (IS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated IS applications, enclaves, outsourced IT-based processes, and platform IT interconnections (reference (d)).

E2.1.23. Information System Security Engineering (ISSE). A sub-discipline under system engineering that considers the value of the information and information assets, threats to and vulnerabilities of those assets, and the affordability of IA solutions. ISSE considers all aspects of IA products, services, measures, and techniques needed to protect ISs and networks using a comprehensive, defense-in-depth approach that integrates the capabilities of personnel, operations, and technology to achieve an appropriate level of protection.

E2.1.24. Integrity. Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (h)).

E2.1.25. Launch Vehicle. The rocket or self-powered portion of the flight component of a space system that is being tested (i.e., research, development, testing, and engineering activities) or otherwise used in an operational context to propel itself or a space platform and its associated mission payload out of the earth's atmosphere.

E2.1.26. Land Remote Sensing Satellite. A satellite that collects data which may be processed into imagery of surface features of the Earth (does not include weather satellites) in accordance with Chapter 82 of title 5, United States Code (U.S.C.) (reference (n)).

E2.1.27. Life Cycle. All phases of a system to include research, planning, concept and architecture definition, design, development, demonstration, test and evaluation, deployment, operations, maintenance, product improvement, and system retirement.

E2.1.28. Mission Assurance Category (MAC). Applicable to DoD ISs, the MAC reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. MACs are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined MACs:

E2.1.28.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and may include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.28.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and may only be tolerated for a short time. The consequences may include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.28.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability may be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences may include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices (reference (d)).

E2.1.29. National Security Information. Information that has been determined, pursuant to Executive Order 12958 (reference (o)) or any predecessor order, to require protection against unauthorized disclosure (reference (h)).

E2.1.30. Non-Repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither may later deny having processed the data (reference (h)).

E2.1.31. NSA-Approved Cryptography. Hardware, firmware, or software implementations of cryptographic algorithms which have been reviewed and approved, or certified and approved by the NSA, the purposes of which are to protect national security or DoD sensitive information or systems in a specific application and intended operational environment.

E2.1.32. Point of Program Initiation. The point within a major defense acquisition program (MDAP) where it is appropriate to require Selective Acquisition Reporting to the Congress and require a formal Acquisition Program Baseline. For DoD Space programs, program initiation typically occurs with the establishment of a System Program Office, and the approval by the DoD Space MDA to proceed into the Design Phase or "Phase B" of a program at the Key Decision Point B Defense Space Acquisition Board in accordance with National Security Space Acquisition Policy 03-01 (reference (p)). For non-MDAP space programs, an equivalent program initiation event shall be used.

E2.1.33. Protected. The appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability in a system that reflect a balance among the value of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; and cost effectiveness.

E2.1.34. Secure Command Destruct System. The cryptographic component of the Flight Termination System. The DIRNSA-approved cryptography incorporated into the launch operations center and launch vehicle that provides a capability for the secure or authenticated transmissions of a flight termination command or the activation the flight termination system (reference (b)).

E2.1.35. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the DCI (reference (h)).

E2.1.36. Sensitive Information. Information whose loss, misuse, or unauthorized access to or modification of may adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (reference (q)), but is not authorized to be kept secret in the interest of national defense or foreign policy under criteria established by an Executive Order or Act of Congress. This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Examples of information to be treated as DoD sensitive include, but are not limited to, the following categories:

E2.1.36.1. For Official Use Only. In accordance with DoD 5400.7-R (reference (r)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (reference (s)).

E2.1.36.2. Unclassified Technical Data. Data related to military or dual-use technology which is subject to approval, licenses or authorization under the Arms Export Control Act (reference (t)) is withheld from public disclosure in accordance with DoD Directive 5230.25 (reference (u)).

E2.1.36.3. Department of State, Sensitive But Unclassified (SBU). Information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security polices.

E2.1.36.4. Foreign Government Information. Information which originated from a foreign government and which is not classified CONFIDENTIAL or higher but must be protected in accordance with DoD 5200.1-R (reference (v)).

E2.1.36.5. Privacy Data. Any record, which is contained in a system of records, as defined in reference (p), and information the disclosure of which may constitute an unwarranted invasion of personal privacy.

E2.1.36.6. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (including security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (w)). Information is designated DoD UCNI only when it is determined that its unauthorized disclosure may reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.36.7. Proprietary Information. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.36.8. Upper-Tier Data and Imagery. Upper-tier data and imagery are those designated under the terms of a commercial remote sensing system operator's license issued under reference (n) as being available only to the USG or to USG-approved customers.

E2.1.36.9. Exclusive USG Use and Access Data and Imagery. Data and imagery from a commercial remote sensing system available exclusively to the USG are those data and imagery designated as upper-tier under the terms of a commercial remote sensing system operator's license issued under reference (n), those data and imagery covered under the terms of a USG order requiring the operator to limit data collection and/or distribution by the system during periods when national security or international obligations may be compromised (commonly referred to as "shutter control" orders), or data and imagery procured under the terms of an exclusive purchase contract. All such data and products are limited to the exclusive use and access by the USG or to USG-approved customers and they require special security and protection measures.

E2.1.37. Space Platform. A satellite, spacecraft or space station developed, launched and operated for purposes of providing specified services to users or customers.

E2.1.38. Space System. All of the devices and organizations forming the space network. These consist of: spacecraft; mission package(s); ground stations; data links among spacecraft, ground stations, and mission or user terminals, which may include initial reception, processing, and exploitation; launch systems; and directly related supporting infrastructure, including space surveillance and battle management and/or command, control, communications, and computers, in accordance with DoD Directive 3100.10 (reference (x)).

E2.1.39. Transmission Security (TRANSEC). Component of communications security resulting from the application of measures designed to protect communications from interception and exploitation by means other than cryptanalysis as defined in (reference (h)).

E2.1.40. Uplink. A data link from a ground or airborne platform to a space platform.

E2.1.41. User Representative. The individual or organization that represents the mission or functional interests of the user community and serves as the liaison for that community throughout the life cycle of the system.

E2.1.42. Vulnerability. Weakness in an IS, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited (reference (h)).

E3. ENCLOSURE 3

FORMAT FOR REQUESTING WAIVERS[8]

(Organization's Letterhead)

DATE:

MEMORANDUM FOR: Director, National Security Agency, Attention: Director for Information Assurance, Suite 6577, 9800 Savage Road, Fort George G. Meade, MD 20755-6577

THRU:
Chain of Command, Address, City, State, Zip Code
Approve_____Disapprove_____
Designated Approving Authority, Address, City, State, Zip Code
Approve_____Disapprove_____

SUBJECT: Waiver to DoD Directive 8581.aa [date], Information Assurance Policy for Space Systems Used by the Department of Defense

1. Request an exception to paragraph x.x.x.

2. Explanatory details: *(Briefly describe pertinent system or mission requirements, capabilities and information assurance concerns, and their relation to waiver.)*

3. Justification for exception: *(The justification shall include acknowledgement that the organization has assessed the threats, vulnerabilities, and overall risk associated with the waiver.)*

4. Impact if waiver is not granted: *(Provide a succinct impact statement describing the impact on operations if the wavier is not granted.)*

5. Point of Contact for Waiver:

Signature Block

i

[8] Waiver requests may be mailed, faxed, or emailed through channels appropriate for the classification level. Contact the intended recipients for current fax numbers or email addresses.